Procedures for Acceptable Use of Electronic Systems

The following requirements must be met in order to receive or maintain an individual electronic system user account:

1. Staff must participate in an annual building or district inservice that reviews Policy No. 2022, Acceptable Use of Electronic Systems.
2. Staff and students must complete the appropriate electronic information system user consent form and agree to abide by the regulations as set forth by board policy. It should be noted that signature on the form acknowledges that the policies and procedures may be subject to change.
    - Students will not be given Internet access without their parent/guardian signature. The parent/guardian will receive a copy of the Acceptable Use of Electronic Systems Policy with the student consent form.
    - Upon registering in the Lynden School District for the first time and at each school transition (grades 6 and 9), parents/guardians will receive a copy of the Acceptable Use Policy and Guidelines with a parent/student consent form. These forms are required in order for students to have internet and/or account privileges.
    - All students at LMS and LHS will be issued an individual student account. An individual student account allows the student access to the Internet, local network services and storage space on the network.
    - If the parent does not want his/her child to have Internet Access or an individual student account, an opt out form is available online or in the school offices. **Opt outs remain in effect for the current school year and must be renewed at the start of each school year.**
3. Students with Internet access must participate in an annual review of Policy No. 2022, Acceptable Use of Electronic Systems.

Electronic System Acceptable Use Guidelines

All student use of the system must be with the approval and/or under the direct supervision of a staff member of the Lynden School District.

All use of the system must be in support of education and research and be consistent with the mission of the district. The district reserves the right to prioritize uses and access to the system.

Any use of the system must conform to state and federal law, network provider policies and licenses, and district policy. Examples include:

- The system constitutes public facilities and may not be used to support or oppose political candidates, groups, or ballot measures.
- Use of the system for charitable purposes must be approved in advance by the superintendent or designee.
- Use of the system for non-district commercial purposes or solicitations is prohibited.
- Authorized software shall only be made available by a member of the technology staff. The unauthorized installation, use, storage, or distribution of copyrighted software and/or materials on district computers is prohibited. Individuals not in compliance with software licensing agreements will be fully responsible for any sanctions or fines incurred from the installation of unlicensed software.

The following activities are prohibited on school district computers unless activities are curriculum based and have received prior approval:

- Gambling software of any kind, local or networked
- Game servers and downloaded games and installed games
- Music servers and downloaded music
- Video/Audio servers and downloaded video/audio
- Auction sites such as EBAY
- BLOGS
- Online radio stations at any time
- Use of the Internet for personal purchase or access to information requiring credit card authorization
- No purchasing for district purposes may be transacted on-line without prior administrative approval.
- Subscriptions to, or use of, mailing lists, bulletin boards, chat groups and commercial on-line services and other information services must be pre-approved by the superintendent or designee.

No use of the system shall serve to disrupt the operation of the system by others. System components including hardware, software, property or facilities shall not be destroyed, modified, or abused in any way. Examples include: tampering or altering security codes or passwords, hacking, introduction of viruses, altering, dismantling, or disfiguring any file data, including without limitation student data, district, school or staff files, and downloading information or messages without authority.

Malicious use of the system to develop programs that harass other users, to gain unauthorized access to any computer or computing system, and/or to damage the components of a computer or computing system is prohibited.

Users are responsible for the appropriateness and content of public and private material transmitted or published on the system. Consistent with the district's harassment-free environment policies, hate mail, harassment, discriminatory remarks, unwelcome compliments or other anti-social behaviors or expressions are prohibited.

Use of the system to access, store or distribute obscene, pornographic or inappropriately suggestive materials is prohibited.

Students, staff members, or patrons wishing to access the Internet must have a signed individual user release form on file with the district. This is required prior to the use of any resource that must be accessed through the use of the Internet. Students must have the approval of a parent/guardian to become an authorized user on the Internet system. This provision applies to access or use by an individual on either a district or personally owned computer.

Security Guidelines

System accounts are to be used only by the authorized user of the account for the authorized purpose. Users may not share their account number or password with another person or leave an open file or session unattended or unsupervised. Users are responsible for all activity under their account. There is no reasonable expectation of personal privacy in the use of account files. Such files are district property and are subject to regular review and monitoring to ensure the responsible use of electronic files consistent with the terms of this policy.

Users shall not seek information, obtain copies of, or modify files or passwords, or use any other means to gain unauthorized access to district systems and information.

Communications may not be encrypted in order to avoid reviews for security and policy violations.

Personal Security Guidelines

Users should never reveal personal information, their own or others, such as home addresses and telephone numbers. All users shall not disclose, use, or disseminate personal identification regarding minors without authorization.

Student users should never meet people in person that they have contacted on the Internet without parent/guardian permission.

Users, including students, are required to notify their teacher, adult, or district representative whenever they come across information or messages that are dangerous,

inappropriate, or make them feel uncomfortable on the web or when using electronic mail or other forms of direct network communications.

Filtering and Monitoring

Filtering software or services must be installed and used on all computers with access to the Internet. This software will block or filter access to visual depictions that are obscene, child pornography, or otherwise harmful to minors. When adults are using the Internet, materials that are obscene and child pornography must still be filtered or blocked.

Educational staff will, to the best of their ability, monitor minors' use of the Internet in school and will take reasonable measures to prevent access by minors to inappropriate material on the Internet and World Wide Web (www) and restrict their access to materials harmful to minors.

All students will be educated about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyberbullying awareness and response. Age appropriate materials will be made available for use across grade levels.

Any attempt to bypass, circumvent, or render inactive or ineffective any access controls or filtering mechanisms will result in cancellation of privileges and subject the member to further disciplinary action according to school and District policies.

District Rights

Lynden School District reserves the right to:

- Review and monitor, as appropriate, all activity on the system for responsible use consistent with the terms of the policy and procedures.
- Make determinations on whether specific uses of the system are consistent with these acceptable use guidelines.
- Temporarily disable an account when investigating suspected inappropriate use.
- Remove a user's access to the system, with notice, at any time the district determines that the user is engaged in unauthorized activity or violating this policy. In addition, further disciplinary or corrective action(s) may be imposed for violations of the policy up to and including termination of employment for staff or appropriate disciplinary sanctions for students.
- Cooperate fully with law enforcement investigation concerning or relating to any suspected or alleged inappropriate activities on the system or any other electronic media.
- Modify, delete, or otherwise change these guidelines and procedures as necessary. This policy will be reviewed every 6 months for the first year after adoption and annually thereafter.

Sanctions for Violations

Disciplinary action, if any, for the students, staff, and other users shall be consistent with the district's standard policies and procedures. Violations of the policy can constitute cause for revocation of access privileges, suspension of access to Lynden School District electronic equipment, other employee or school disciplinary action, and/or other appropriate legal or criminal action, including restitution, if appropriate. Students shall be subject to the sanctions of WAC 180-40, et. seq., as appropriate.

From time to time the district will make a determination on whether specific uses of the K-20 Network are consistent with the regulations stated above. Under prescribed circumstances non-student or non-staff use may be permitted, provided such individuals demonstrate that their use furthers the purpose and goals of the district. For security and administrative purposes the district reserves the right for authorized personnel to review network use and content. The district reserves the right to remove an individual's network access privileges to prevent further unauthorized activity.

Revised: June 17, 1999
Revised: June 23, 2005
Revised: May 26, 2011
Revised: March 22, 2012